대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0045216
Application Number

출 원 년 월 일 : 2003년 07월 04일
Date of Application JUL 04, 2003

출 원 인 : 학교법인 한국정보통신학원
Applicant(s) INFORMATION AND COMMUNICATIONS UNIVERSITY EDUCA

2003 년 10 월 23 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【참조번호】 0001
【제출일자】 2003.07.04
【발명의 명칭】 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치 및 방법
【발명의 영문명칭】 APPARATUS AND METHOD FOR GENERATING AND VERIFYING ID-BASED BLIND SIGNATURE BY USING BILINEAR PARINGS
【출원인】
【명칭】 학교법인 한국정보통신학원
【출원인코드】 2-1999-038195-0
【대리인】
【성명】 장성구
【대리인코드】 9-1998-000514-8
【포괄위임등록번호】 2000-005740-6
【대리인】
【성명】 김원준
【대리인코드】 9-1998-000104-8
【포괄위임등록번호】 2000-005743-8
【발명자】
【성명의 국문표기】 장 팡구오
【성명의 영문표기】 ZHANG,Fangguo
【주민등록번호】 000000-0000000
【우편번호】 305-732
【주소】 대전광역시 유성구 화암동 58-4
【국적】 KR
【발명자】
【성명의 국문표기】 김광조
【성명의 영문표기】 KIM,Kwangjo
【주민등록번호】 560410-1347622
【우편번호】 305-348
【주소】 대전광역시 유성구 화암동 58-4
【국적】 KR

【발명자】

【성명의 국문표기】	최형기
【성명의 영문표기】	CHOI,Hyunggi
【주민등록번호】	740109-1063425
【우편번호】	305-732
【주소】	대전광역시 유성구 화암동 58-4
【국적】	KR
【심사청구】	청구
【조기공개】	신청
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 심사청구 , 특허법 제64조의 규정에 의한 출원공개를 신청합니다. 대리인 장성구 (인) 대리인 김원준 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	4	면	4,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	16	항	621,000 원
【합계】	654,000 원		
【감면사유】	학교		
【감면후 수수료】	327,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통 2.고등교육법 제2조에의한 학교임을 증명하는 서류_1통

【요약서】

【요약】

서명자, 사용자 및 신뢰기관을 참여자로 갖는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치 및 방법에 있어서, 신뢰기관은 시스템 매개변수를 생성하고 마스터키를 선택한다. 또한, 신뢰기관은 서명자의 개인식별정보를 이용하여 서명자의 한 쌍의 공개키와 비밀키를 생성한다. 신뢰기관은 시스템 매개변수와 서명자의 공개키를 포함하는 공개값을 공개하고, 서명자의 비밀키를 안전한 채널을 통해 서명자에게 전송한다. 사용자는 공개값을 수신 및 저장하며 서명자는 공개값과 서명자의 비밀키를 수신 및 저장한다. 서명자는 위탁값을 계산하여 사용자에게 전송하고 사용자는 메시지를 은닉하여 서명자에게 전송한다. 서명자는 은닉 메시지에 서명하여 사용자에게 전송하고 사용자는 서명된 메시지를 복구한다. 마지막으로 사용자는 서명의 정당성을 검증한다.

【대표도】

도 2

【명세서】

【발명의 명칭】

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치 및 방법{APPARATUS AND METHOD FOR GENERATING AND VERIFYING ID-BASED BLIND SIGNATURE BY USING BILINEAR PARINGS}

【도면의 간단한 설명】

도 1a 와 1b는 본 발명의 바람직한 실시예에 따른 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 시스템을 예시하는 블록도.

도 2는 본 발명의 바람직한 실시예에 따른 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 시스템의 작동을 예시하는 흐름도.

<도면의 주요 부분에 대한 부호의 설명>

100 : 서명자 200 : 사용자

300 : 신뢰기관(또는, 키생성 센터)

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<6> 본 발명은 암호 시스템에 관한 것이며, 더욱 상세하게는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 시스템에 관한 것이다.

<7> 공개키 시스템에서, 각 사용자는 공개키와 비밀키 쌍을 갖는다. 사용자의 공개키와 개인식별정보의 연결은 전자 인증서(Digital Certificate)에 의한다. 인증서 기반 시스템(certificate based system)에서, 사용자의 공개키를 사용하기 전에 참여자는 먼저 사용자의 인증서를 검증해야 한다. 따라서, 사용자의 수가 급속히 증가함에 따라 인증서 기반 시스템은 많은 양의 계산 시간과 저장 공간을 요구한다.

<8> 인증서 기반의 공개키 셋팅에서 키관리 절차를 단순화하기 위하여, 샤미르(Shamir)는 1984년에 개인식별정보 기반의 암호화 기법과 서명 기법을 제안했다(A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.). 그 후로 많은 개인식별정보 기반의 암호화 기법과 서명 기법이 제안되었다. 개인식별정보 기반의 암호시스템의 중요한 아이디어는 각각의 사용자를 식별할 수 있는 정보가 사용자의 공개키로 사용되어지는 것을 말한다. 다시 말하자면 사용자의 공개키가 인증발급기관으로부터 발행된 인증서로부터 공개키를 추출하여 사용하는 대신에 직접적으로 사용자의 공개키로 계산 될 수 있다는 것을 뜻한다. 따라서, 개인식별정보 기반의 공개키 구조는 인증서를 기반으로 하는 공개키 구조를 효과적으로 대체 할 수 있는 기법이고 효율적인 키 관리와 일반적인 보안요구도가 필요한 시스템에 적절하다.

<9> 겹선형쌍(bilinear pairs), 예를 들면, 대수 곡선의 웨일(Weil) 쌍과 테이트(Tate) 쌍은 대수기하학 연구에서 매우 중요한 도구들이다. 암호 시스템에서 겹선형쌍 성질의 초기 응용은 이산대수문제(Discrete Logarithm Problem)를 평가하기 위해 이용되었다. 예를 들면, 웨일 쌍을 사용한 엠오브이(MOV) 공격이나 테이트 쌍을 이용한 에프알(FR) 공격은 특정 타원곡선이나 초타원곡선에서의 이산대수문제를 유한체에서의 이산대수문제로 축약하였다. 최근에는 이러한 겹선형쌍이 암호학에서 다양하게 응용될 수 있다는 것이 밝혀졌다. 더욱 정확하게는 겹선형쌍들은 개인식별정보 기반의 암호 시스템을 구축하는데 사용될 수 있다. 많은 개인식별정보 기반의 암호 시스템이 겹선형쌍을 이용하여 제안되었다.

<10> 예를 들면 보네(Boneh)와 프랭크린(Franklin)의 개인식별정보 기반 암호 시스템(D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.)과 스마트(Smart)의 개인식별정보 기반 인증 키 합의 프로토콜(N.P. Smart, Identity-based authenticated key agreement protocol based on Weil pairing, Electron. Lett., Vol.38, No.13, pp.630-632, 2002.) 및 몇 가지 개인식별정보 기반 서명 기법이 있다.

<11> 공개키 셋팅에서 사용자의 익명성은 은닉서명에 의해 보호된다. 은닉서명의 개념은 촘(D. Chaum, Blind signatures for untraceable payments, Advances in Cryptology Crypto 82, Plenum, NY, pp.199-203, 1983.)에 의해서 최초로 제안되었으며, 전자 투표 및 전자 결재 시스템 등과 같은 응용 시스템에서 사용자의 익명성을 제공한다. 일반 전자서명과 달리, 은닉서명은 사용자와 서명자간의 2자간 대화형 프로토콜이라 볼 수 있다. 은닉서명을 이용해 사용자는 서명자가 메시지와 서명 결과에 대한 정보를 얻을 수 없는 채로 메시지의 서명 값을 얻을 수 있다. 은닉서명은 익명성의 전자 화폐 시스템을 구축하는데 중요한 역할을 담당한다.

<12> 최근에 겹선형쌍을 이용한 개인식별정보 기반의 전자 서명 시스템이 몇 가지 개발되었다. 개인식별정보 기반의 은닉 서명은 개인의 공개키가 단순히 그의 개인식별정보인 것이 장점이다. 예를 들어, 은행이 개인식별정보 기반의 은닉 서명으로 전자 화폐를 발행한다면, 사용자나 상점은 데이터베이스에서 은행의 공개키를 가져올 필요가 없다. 그들은 국가명, 도시명, 은행 이름, 해당 년도 등의 연접 정보를 통해서 당해 년도에 발행된 전자현금을 쉽게 검증할 수 있다.

【발명이 이루고자 하는 기술적 과제】

<13> 일반적인 은닉 서명 시스템은 많은 양의 계산 시간과 저장 공간을 요구하지만, 개인식별정보 기반의 은닉 서명은 개인의 공개키가 단순히 그의 개인식별정보이기 때문에 계산 시간과 저장 공간을 줄일 수 있다. 또한, 본 발명의 은닉 서명 시스템은 사용자의 익명성 뿐만 아니라 위조불가능성도 만족하면서, 제네릭 패러렐 공격(generic pararrel attack) 에 대한 안전성에 대해서 알오에스(ROS) 문제의 어려움을 기반으로 하지 않는다.

<14> 본 발명의 일 측면에 의하면, 서명자, 사용자 및 신뢰기관을 참여자로 갖는 개인식별정보 기반의 은닉서명 장치에 있어서, 상기 신뢰기관이 시스템 매개변수를 생성하고 마스터키를 선택하는 수단과, 상기 신뢰기관이 상기 서명자의 개인식별정보를 이용하여 상기 서명자의 한 쌍의 공개키와 비밀키를 생성하는 수단과, 상기 신뢰기관이 상기 시스템 매개변수와 상기 서명자의 공개키를 포함하는 공개값을 공개하는 수단과 상기 서명자의 비밀키를 안전한 채널을 통해 상기 서명자에게 전송하는 수단과, 상기 사용자가 상기 공개값을 수신하고 저장하는 수단과 상기 서명자가 상기 공개값과 상기 서명자의 비밀키를 수신하고 저장하는 수단과, 상기 서명자가 위탁 값을 계산하고 상기 위탁 값을 상기 사용자에게 전송하는 수단과, 상기 사용자가 메

시지를 은닉하고 상기 은닉 메시지를 서명자에게 전송하는 수단과, 상기 서명자가 상기 은닉 메시지에 서명하고 상기 서명된 메시지를 상기 사용자에게 전송하는 수단과, 상기 사용자가 상기 서명된 메시지를 복구하는 수단과, 상기 사용자가 서명의 정당성을 검증하는 수단을 포함하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치가 제공된다.

<15> 본 발명의 또 다른 측면에 의하면, 서명자, 사용자 및 신뢰기관을 참여자로 갖는 개인식별정보 기반의 은닉서명 방법에 있어서, 상기 신뢰기관이 시스템 매개변수를 생성하고 마스터키를 선택하는 단계와, 상기 신뢰기관이 상기 서명자의 개인식별정보를 이용하여 상기 서명자의 한 쌍의 공개키와 비밀키를 생성하는 단계와, 상기 신뢰기관이 상기 시스템 매개변수와 상기 서명자의 공개키를 포함하는 공개값을 공개하는 단계와 상기 공개값과 상기 서명자의 비밀키를 안전한 채널을 통해 상기 서명자에게 전송하는 단계와, 상기 사용자가 상기 공개값을 수신하고 저장하는 단계와 상기 서명자가 상기 공개값과 상기 서명자의 비밀키를 수신하고 저장하는 단계와, 상기 서명자가 위탁 값을 계산하고 상기 위탁 값을 상기 사용자에게 전송하는 단계와, 상기 사용자가 메시지를 은닉하고 상기 은닉 메시지를 서명자에게 전송하는 단계와, 상기 서명자가 상기 은닉 메시지에 서명하고 상기 서명된 메시지를 상기 사용자에게 전송하는 단계와, 상기 사용자가 상기 서명된 메시지를 복구하는 단계와, 상기 사용자가 서명의 정당성을 검증하는 단계를 포함하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법이 제공된다.

【발명의 구성 및 작용】

<16> 도 1a는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 시스템의 블록도이다. 본 시스템은 서명자(100), 사용자(200), 신뢰기관(300)의 세 참여자를 포함한다. 여기서 본 시스템의 각 참여자는 컴퓨터 시스템일 수 있으며, 임의의 종류의 통신 네트워크 또는 다른 기술에

의해 원격으로 통신할 수 있다. 참여자들 사이에 전송될 정보는 다양한 형태의 저장 매체에 저장되거나 기억될 수 있다.

<17> 신뢰기관(300)은 시스템 매개변수를 생성하고 마스터키를 선택한다. 또한, 신뢰기관(300)은 서명자의 개인식별정보를 사용하여 서명자(100)의 공개키와 비밀키 쌍을 생성한다. 그리고 신뢰기관(300)은 시스템 매개변수와 서명자의 공개키를 포함하는 공개값을 공개하고, 서명자(100)의 비밀키를 안전한 채널을 통해 서명자(100)에게 전송한다.

<18> 사용자(200)는 신뢰기관(300)이 제공하는 공개값을 수신 및 저장한다. 그리고 사용자(200)는 그것을 저장매체에 저장하거나 기억한다.

<19> 그 동안, 서명자(100)는 신뢰기관(300)이 제공하는 공개값과 서명자의 비밀키를 수신 및 저장한다. 그리고 서명자(100)는 그것을 저장매체에 저장하거나 기억한다.

<20> 도 1b는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 시스템에 참여하는 서명자(100)와 사용자(200)의 블록도이다. 서명자(100)는 위탁 값을 계산하여 그 위탁 값을 사용자(200)에게 전송한다. 사용자(200)는 서명될 메시지를 은닉하여 그 은닉 메시지를 서명자(100)에게 전송한다. 서명자(100)는 메시지의 내용을 모른 채 은닉 메시지의 서명 값을 계산하여 사용자(200)에게 전송한다. 마지막으로, 사용자(200)는 서명자(100)로부터 서명된 메시지를 수신하여 서명의 정당성을 검증한다.

<21> 이제 도 2를 참조하여, 본 발명에 따른 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법에 대해 상세하게 설명한다.

<22> G_1 은 생성자 P 에 의해서 생성되는 위수가 q 인 순환군이고, G_2 는 동일한 위수 q 를 갖는 곱셈 순환군이다. G_1 과 G_2 에서 이산 대수 문제는 복잡하다. $e: G_1 \times G_1 \rightarrow G_2$ 는 다음의 조건을 만족시키는 겹선형 사상이다.

<23> 1. $e(aP, bQ) = e(P, Q)^{ab}$ 를 만족하는 겹선형성

<24> 2. $e(P, Q) \neq 1$ 을 만족하는 $P, Q \in G_1$ 의 존재성

<25> 3. 모든 $P, Q \in G_1$ 에 대한 $e(P, Q)$ 계산의 효율성

<26> 시스템 매개변수를 생성하는 과정(단계 201) 동안 위수 q 인 순환군 G_1 과 G_2 가 생성된다. 그리고 순환군 G_1 의 생성자인 P 와 두 순환군 G_1 과 G_2 에 대한 겹선형 사상 $e: G_1 \times G_1 \rightarrow G_2$ 를 생성한다. 본 발명에서 G_1 은 타원 곡선군 또는 초타원 곡선 자코비언(Jacobian)이며, G_2 는 곱셈 순환군 Z_q^* 을 사용한다. 다음으로, 신뢰 기관(300)은 마스터키로 Z_q^* 에 속하는 임의의 정수 s 를 선택하고 $P_{pub} = s \cdot P$ 을 계산한다. 추가로, 암호학적 해시 함수 $H_1: \{0,1\}^* \rightarrow Z_q^*$ 와 $H_2: \{0,1\}^* \rightarrow G_1$ 를 선택한다.

<27> 그 후에 신뢰기관(300)은 서명자(100)의 개인식별정보를 사용하여 서명자(100)의 비밀키와 공개키쌍을 생성한다(단계 202). 서명자의 개인식별정보 ID 가 주어지면, 신뢰기관(300)은 공개키 $Q_{ID} = H_2(ID)$ 와 비밀키 $S_{ID} = s \cdot Q_{ID}$ 를 반환한다.

<28> 신뢰기관(300)은 서명자(100)와 사용자(200)가 공유할 $<G_1, G_2, e, q, P, P_{pub}, H_1, H_2>$ 을 시스템 매개변수로서 공개한다. 또한 신뢰기관(300)은 서명자(100)의 공개키를 공개하고 서명자(100)의 비밀키를 안전한 채널을 통해 서명자(100)에게 전송한다(단계 203).

<29> 은닉 서명 과정에서, 서명자(100)는 Z_q^* 에 속하는 난수 r 을 선택하고, $U = r \cdot Q_{ID}$을 계산하여 사용자(200)에게 U 을 위탁값으로 전송한다(단계 204).

<30> 사용자(200)는 은닉 인수로서 Z_q^* 에 속하는 난수 a 와 β를 선택한다. 사용자(200)는 은닉 메시지 $h = a^{-1}H_1(m, U') + \beta$를 계산하여 서명자(100)에게 전송한다(단계 205). 여기서 $U' = aU + a\beta Q_{ID}$ 이고 m 은 서명될 메시지이다.

<31> 서명자(100)는 서명 값 $V = (r + h)S_{ID}$ 을 계산하여 사용자에게 전송한다(단계 206).

<32> 사용자(200)는 사용자(200)가 선택한 은닉 인수를 사용하여 $V' = aV$ 를 계산하여 $\{m, U', V'\}$을 출력한다(단계 208). (U', V') 은 메시지 m 의 은닉 서명 값이다.

<33> 서명 검증의 과정(단계 209)에서, 사용자(200)는 메시지 m 과, 신뢰기관(300)이 공개한 시스템 매개변수와, 서명자의 공개키 Q_{ID} 를 사용한다. 서명은 $e(V', P) = e(U' + H_1(m, U')Q_{ID}, P_{pub})$인 경우에 정당하다. 서명의 정당성은 수학식 1에 의해 정당화된다.

<34> 【수학식 1】 $e(V', P)$

<35> $= e(aV, P)$

<36> $= e((ar + ah)S_{ID}, P)$

<37> $= e((ar + H_1(m, U') + a\beta)Q_{ID}, P_{pub})$

<38> $= e((ar + a\beta)Q_{ID} + H_1(m, U')Q_{ID}, P_{pub})$

<39> $= e(U', + H_1(m, U')Q_{ID}, P_{pub})$

<40> 위에서 언급한 것처럼, 본 발명의 개인식별정보 기반의 은닉서명 기법은 일반적인 은닉서명 기법과 개인식별정보 기반 기법의 조합이다. 즉, 이것은 은닉서명이지만, 검증을 위한 공개키가 단지 서명자의 개인식별정보이다.

<41> 개인식별정보 기반의 은닉서명 기법은 특정타원곡선 또는 초타원곡선상에서 구현될 수 있다. 개인식별정보 기반의 서명 기법에서 가장 중요한 부분은 겹선형쌍을 계산하는 것이다. 겹선형쌍의 계산은 효율적으로 되었으며, 서명의 길이는 압축 기술에 의해 줄어들 수 있다.

<42> 본 발명의 개인식별정보 기반의 은닉서명 기법은 임의의 수가 아닌 개인식별정보에 기반하므로, 공개키는 이메일 주소와 같이 개인을 유일하게 식별시킬 수 있는 개인식별정보로 구성된다. 응용예에서, 공개키와 서명의 길이는 줄어들 수 있다. 예를 들어 전자 투표 시스템 또는 전자 경매 시스템에서, 등록 매니저는 개인식별정보 기반의 암호화 시스템에서의 신뢰기관의 역할을 담당할 수 있다. 등록 단계에서 등록 매니저는 입찰자 또는 투표인에게 그의 등록 번호를 그의 공개키 ={(전자 투표 또는 전자 경매 시스템의 이름 ‖ 등록 매니저 ‖ 날짜 ‖ 숫자), n} 로 제공할 수 있다. 여기서 n 은 모든 입찰자 또는 투표자의 수이다.

<43> 게다가, 본 발명의 은닉서명을 사용하면 사용자의 익명성과 위조불가능성을 제공할 수 있다. 그룹 G_1상에서 *Pa*를 겹선형 쌍계산이라고 하고, *Pm*을 스칼라 곱셈, *Ad*를 스칼라 덧셈, *Mu*를 Z_q상에서의 곱셈, 그리고 *Div*를 Z_q상에서의 나눗셈, 그리고 *MuG2*를 G_2상에서 곱셈이라고 했을 때, 본 발명은 사용자가 *3Pm + 1Ad + 1Mu + 1Div*, 서명자가 *2Pm*, 검증 단계에서는 *2Pa + 1Pm + 1Ad* 의 계산을 필요로 하고 있다. 계산 양을 볼 때 본 발명이 효율적이라는 것을 쉽게 확인 할 수 있다. 검증이 자주 일어난다면 수학식 2(batch verification)을 이용하여 계산하여 효율성을 높일 수 있다.

<44> 【수학식 2】 $$e(\sum_{i=1}^{n} V_i', P) = e(\sum_{i=1}^{n} U_i' + (\sum_{i=1}^{n} H_1(m_i, U_i'))Q_{ID}, P_{pub})$$

<45> 위에서 설명한 본 발명에 따른 겹선형쌍을 이용한 개인식별정보 기반의 은닉 서명 시스템은 계산 시간과 저장 용량을 줄일 수 있으며, 키 관리 절차를 단순화시킬 수 있다. 개인의

공개키는 단순히 그의 개인식별정보이기 때문에, 다른 사람은 데이터베이스에게 그의 공개키를 가져올 필요가 없다. 따라서, 개인식별정보 기반의 공개키 셋팅은 인증서 기반의 공개키 셋팅의 대안이 될 수 있다.

<46> 앞서 기술한 것은 본 발명의 특정한 실시예에 대한 기술과 설명일 뿐이므로, 당업자는 다음 청구항에 정의된 본 발명의 범위와 본질에서 벗어남이 없이 다양한 변형과 변화를 거기에 가할 수 있다.

【발명의 효과】

<47> 따라서, 본 발명의 주 목적은 계산 시간과 저장 공간을 감소시키고 키관리 절차를 단순화시키는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치 및 방법을 제공하는데 있다. 본 발명의 은닉 서명 시스템은 사용자의 익명성 뿐만 아니라 위조불가능성도 만족하면서, 제네릭 패러렐 공격(generic pararrel attack) 에 대한 안전성에 대해서 알오에스(ROS) 문제의 어려움을 기반으로 하지 않고 효율적인 은닉 서명을 수행할 수 있다.

【특허청구범위】

【청구항 1】

서명자, 사용자 및 신뢰기관을 참여자로 갖는 개인식별정보 기반의 은닉서명 장치에 있어서,

상기 신뢰기관이 시스템 매개변수를 생성하고 마스터키를 선택하는 수단과,

상기 신뢰기관이 상기 서명자의 개인식별정보를 이용하여 상기 서명자의 한 쌍의 공개키와 비밀키를 생성하는 수단과,

상기 신뢰기관이 상기 시스템 매개변수와 상기 서명자의 공개키를 포함하는 공개값을 공개하는 수단과 상기 서명자의 비밀키를 안전한 채널을 통해 상기 서명자에게 전송하는 수단과,

상기 사용자가 상기 공개값을 수신하여 저장하는 수단과 상기 서명자가 상기 공개값과 상기 서명자의 비밀키를 수신하여 저장하는 수단과,

상기 서명자가 위탁 값을 계산하고 상기 위탁 값을 상기 사용자에게 전송하는 수단과,

상기 사용자가 메시지를 은닉하고 상기 은닉 메시지를 서명자에게 전송하는 수단과,

상기 서명자가 상기 은닉 메시지에 서명하고 상기 서명된 메시지를 상기 사용자에게 전송하는 수단과,

상기 사용자가 상기 서명된 메시지를 복구하는 수단과,

상기 사용자가 서명의 정당성을 검증하는 수단을 포함하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치.

【청구항 2】

제 1 항에 있어서,

상기 시스템 파라미터는 순환군 G_1, 곱셈 순환군 G_2, 겹선형쌍 e, 상기 G_1 의 위수 q, 상기 G_1 의 생성자 P, 상기 신뢰기관의 공개키 P_{pub} 과 해시 함수 H_1 및 H_2 을 포함하되,

G_2는 상기 위수 q를 갖는 곱셈 순환군으로서 곱셈순환군 Z_q^* 을 사용하고, 상기 겹선형쌍은 $e: G_1 \times G_1 \rightarrow G_2$ 로 정의되고, 상기 신뢰기관의 공개키는 마스터키 s 를 사용하여 $P_{pub} = s \cdot P$ 로 계산되며, 상기 해시 함수는 $H_1: \{0,1\}^* \rightarrow Z_q^*$ 와 $H_2: \{0,1\}^* \rightarrow G_1$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치.

【청구항 3】

제 2 항에 있어서,

상기 서명자의 공개키 Q_{ID} 는 상기 서명자의 개인식별정보 ID 를 사용하여 $Q_{ID} = H_2(ID)$ 로 계산되며,

상기 서명자의 비밀키 S_{ID} 는 $S_{ID} = s \cdot Q_{ID}$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치.

【청구항 4】

제 3 항에 있어서,

상기 위탁 값 U 은 상기 서명자가 선택한 난수 r 를 사용하여 $U = r \cdot Q_{ID}$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치.

【청구항 5】

제 4 항에 있어서,

상기 은닉 메시지 h 는 보내려는 메시지 m 와 Z_q^* 에 속하는 은닉 인수 a 및 β 를 사용하여 $h = a^{-1}H_1(m, U') + \beta$, $U' = aU + a\beta Q_{ID}$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치.

【청구항 6】

제 5 항에 있어서,

상기 서명된 메시지는 $V = (r + h)S_{ID}$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치.

【청구항 7】

제 6 항에 있어서,

상기 서명된 메시지를 복구하는 수단은 $V' = aV$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치.

【청구항 8】

제 7 항에 있어서,

상기 서명의 정당성을 검증하는 수단은 다음의 수학식으로 수행되는 것을 특징으로 하는

$$e(V', P)$$

$$= e(aV, P)$$

$$= e((ar + ah)S_{ID}, P)$$

$$= e((ar + H_1(m, U') + a\beta)Q_{ID}, P_{pub})$$

$$= e((ar + a\beta)Q_{ID} + H_1(m, U')Q_{ID}, P_{pub})$$

$$= e(U', + H_1(m, U')Q_{ID}, P_{pub})$$

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 장치.

【청구항 9】

서명자, 사용자 및 신뢰기관을 참여자로 갖는 개인식별정보 기반의 은닉서명 방법에 있어서,

상기 신뢰기관이 시스템 매개변수를 생성하고 마스터키를 선택하는 단계와,

상기 신뢰기관이 상기 서명자의 개인식별정보를 이용하여 상기 서명자의 한 쌍의 공개키와 비밀키를 생성하는 단계와,

상기 신뢰기관이 상기 시스템 매개변수와 상기 서명자의 공개키를 포함하는 공개값을 공개하는 단계와 상기 서명자의 비밀키를 안전한 채널을 통해 상기 서명자에게 전송하는 단계와,

상기 사용자가 상기 공개값을 수신하여 저장하는 단계와 상기 서명자가 상기 공개값과 상기 서명자의 비밀키를 수신하여 저장하는 단계와,

상기 서명자가 위탁 값을 계산하고 상기 위탁 값을 상기 사용자에게 전송하는 단계와,

상기 사용자가 메시지를 은닉하고 상기 은닉 메시지를 서명자에게 전송하는 단계와,

상기 서명자가 상기 은닉 메시지에 서명하고 상기 서명된 메시지를 상기 사용자에게 전송하는 단계와,

상기 사용자가 상기 서명된 메시지를 복구하는 단계와,

상기 사용자가 서명의 정당성을 검증하는 단계를 포함하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 10】

제 9 항에 있어서,

상기 시스템 파라미터는 순환군 G_1, 곱셈 순환군 G_2, 겹선형쌍 e, 상기 G_1 의 위수 q, 상기 G_1 의 생성자 P, 상기 신뢰기관의 공개키 P_{pub} 과 해시 함수 H_1 및 H_2 을 포함하되,

G_2는 상기 위수 q를 갖는 곱셈 순환군으로서 곱셈순환군 Z_q^* 을 사용하고, 상기 겹선형 쌍은 $e: G_1 \times G_1 \rightarrow G_2$ 로 정의되고, 상기 신뢰기관의 공개키는 마스터키 s 를 사용하여 $P_{pub} = s \cdot P$ 로 계산되며, 상기 해시 함수는 $H_1: \{0,1\}^* \rightarrow Z_q^*$ 와 $H_2: \{0,1\}^* \rightarrow G_1$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 11】

제 10 항에 있어서,

상기 서명자의 공개키 Q_{ID} 는 상기 서명자의 개인식별정보 ID 를 사용하여 $Q_{ID} = H_2(ID)$ 로 계산되며,

상기 서명자의 비밀키 S_{ID} 는 $S_{ID} = s \cdot Q_{ID}$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 12】

제 11 항에 있어서,

상기 위탁 값 U 은 상기 서명자가 선택한 난수 r 를 사용하여 $U = r \cdot Q_{ID}$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 13】

제 12 항에 있어서,

상기 은닉 메시지 h 는 보내려는 메시지 m 와 Z_q^* 에 속하는 은닉 인수 a 및 β 를 사용하여 $h = a^{-1}H_1(m, U') + \beta$, $U' = aU + a\beta Q_{ID}$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 14】

제 13 항에 있어서,

상기 서명된 메시지는 $V = (r + h)S_{ID}$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 15】

제 14 항에 있어서,

상기 서명된 메시지를 복구하는 단계는 $V' = aV$ 로 계산되는 것을 특징으로 하는

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 16】

제 15 항에 있어서,

상기 서명의 정당성을 검증하는 단계는 다음의 수학식으로 수행되는 것을 특징으로 하는

$e(V', P)$

$= e(\alpha V, P)$

$= e((\alpha r + \alpha h)S_{ID}, P)$

$= e((\alpha r + H_1(m, U') + \alpha \beta)Q_{ID}, P_{pub})$

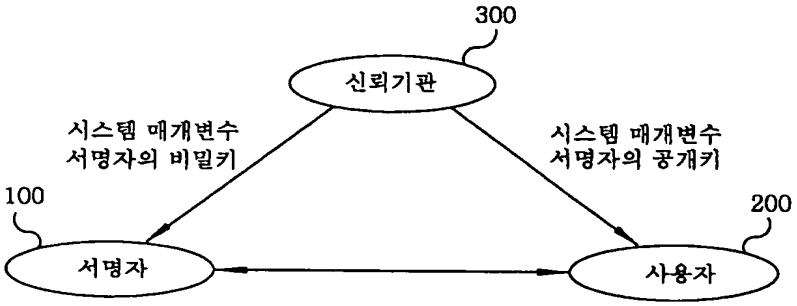
$= e((\alpha r + \alpha \beta)Q_{ID} + H_1(m, U')Q_{ID}, P_{pub})$

$= e(U', + H_1(m, U')Q_{ID}, P_{pub})$

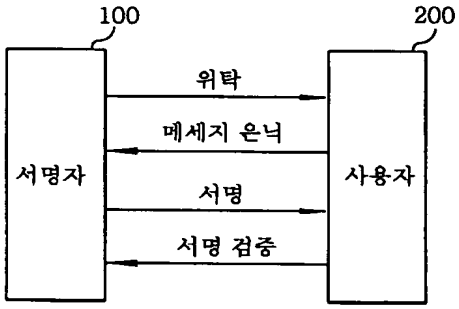
겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【도면】

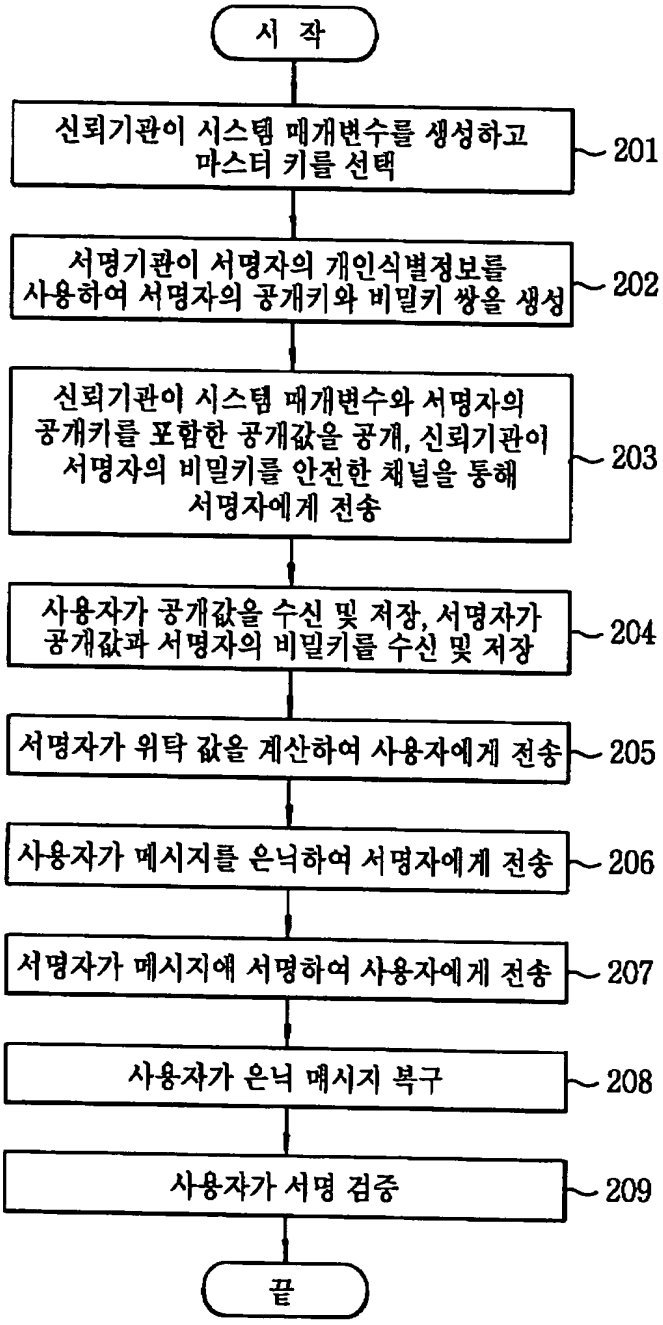
【도 1a】


300
신뢰기관
시스템 매개변수
서명자의 비밀키
시스템 매개변수
서명자의 공개키
100
200
서명자
사용자

【도 1b】


100
200
서명자
사용자
위탁
메세지 온닉
서명
서명 검증

【도 2】


시 작
신뢰기관이 시스템 매개변수를 생성하고 마스터 키를 선택
201
서명기관이 서명자의 개인식별정보를 사용하여 서명자의 공개키와 비밀키 쌍을 생성
202
신뢰기관이 시스템 매개변수와 서명자의 공개키를 포함한 공개값을 공개, 신뢰기관이 서명자의 비밀키를 안전한 채널을 통해 서명자에게 전송
203
사용자가 공개값을 수신 및 저장, 서명자가 공개값과 서명자의 비밀키를 수신 및 저장
204
서명자가 위탁 값을 계산하여 사용자에게 전송
205
사용자가 메시지를 은닉하여 서명자에게 전송
206
서명자가 메시지에 서명하여 사용자에게 전송
207
사용자가 은닉 메시지 복구
208
사용자가 서명 검증
209
끝